d.) Remarks

The present invention introduces the concept of using graphic objects displayed visually onscreen as passwords to protect other objects displayed visually onscreen, a process that improves upon and replaces the typical alphanumeric password scheme used in prior art computing systems. Graphic objects such as photos, pictures, drawings, color lines of various hues and combination, and the like are password keys that are far more difficult to guess or decipher through brute force computing than simple strings of alphanumeric characters.

In the invention, any visually displayed onscreen object may be designated as a password for any further onscreen object. After the designated password object is applied to the further onscreen object, the further onscreen object becomes a protected object that cannot be accessed unless and until the password object is first used to unlike the further object. Applying the designated password object may be accomplished graphically by dragging it over the further onscreen object, or by the use of an arrow drawn from the password object to the further object, or the like. Thereafter the association of the password object as the protection key of the protected object is not evident in any way. The password key may be applied by once again calling forth the display of the password object, and thereafter dragging the password object over the protected object.

The protected object may contain a data file, a function device such as a video mixer or audio sequencer, an image or photo, a secret text file, or the like. Whatever it contains, its contents and function cannot be accessed until the password key is applied as described above. A further aspect of the invention is that a grouping of two or more visually displayed onscreen objects may be selected and joined together to form a single password object, thereby further increasing the combinatorial possibilities of the password key. As described in the specification, an image or photo may include drawn lines of particular hues or colors that are difficult to notice visually against the image background, but are critical to the combined function as a password key. Many similar combinations of visual elements are described in the specification and drawings of the application.

In the instant Action the rejection of all claims under §102 and §103 is based primarily on the Arsenault reference, US patent no. 6,870,546. Arsenault is directed toward the creation and protection of shape designs authored in a CAD application program or the like. As shown in Figure 2 of the reference, the shape object 200 is protected by a protection object 220. The protection object 220 governs the protection of property values and property expressions for all properties of the shape object 200. Once the protection object 220 turns on protection for an object 200, users of the shape object are prevented from examining and modifying the values and expressions of the properties of the shape object.

When Arsenault makes reference to graphic objects, it is referring to the shape designs that are to be protected. Note the col. 5 (lines 10 et seq.) citation in the rejection: " As an example, consider an object 200 (e.g., a shape object 200) that describes a chair. Such an object 200 has a geometry, which describes the paths used to render the appearance of the chair on a page. The object 200 may be composed of geometry that describes the chair's support members, with sub-shapes making up the seat, back, arms and other elements (and each of those shapes have their own properties, and so on)." Clearly Arsenault is involved with protecting elements and sub-elements that are geometric.

However, the scheme for protecting the shape designs does NOT involve any graphic elements as keys or passwords. As described in col. 8, lines12-20, "the protection object 220 may have one or more of the following properties and/or methods:

(1) a parent property

(2) a universal identification property;

(3) a make universal identification method;

(4) a set password method;

(5) a clear password method; and

(6) a has password method."

It is significant to note that "graphic" is never mentioned in describing the protection object 220. That is due to the fact that the protection object is NOT a graphic object; it has no graphic definition, no graphic presence, and no graphic characteristics. Rather, it is an "object" only within the framework of an object oriented program (OOP); that is, it consists of a class definition and depending data elements that define the object as a specific member of the defined class. Indeed, col. 8, line 21-col. 9, line 37 of Arsenault describe the six properties above in terms that are a clear indication of the OOP nature of the protection object.

Note, for example, that the universal identification property is defined in col. 8, line 35 as an alphanumeric string of a particular serial character format, which bears no relationship to a graphic object that is capable of being displayed onscreen and used as a password. Likewise, the set password and clear password methods involve a 16 byte data block, which is a literal alphanumeric string, NOT a graphic object.

It is also significant that Figure 6 of Arsenault, which depicts the flow chart of the protection scheme of the reference, makes absolutely no suggestion or allusion to the use of graphic objects displayed onscreen and designated as a password to protect some other onscreen object.

Looking at the totality of Arsenault, it is clear that the reference lacks any teaching that relates to the core idea of the invention as described and claimed. Thus Arsenault fails as a reference, both under §102 for anticipation and under §103 for obviousness.

The Yarsa patent is combined with Arsenault to reject claims 12 and 13 under §103(a). Yarsa does teach a technique to verify the data integrity of a PFX object (again, an OOP object, as evidenced by the name field, version field, integrity mode field, etc., of the PFX object) by drag-and-drop of an icon representing a public cryptographic key or an encoded certificate over the PFX object. However, this teaching does not bolster the inadequate Arsenault teaching, since neither reference reveals or suggests the use of the complexities of a visually displayed graphic object to form a password that has enormous combinatorial possibilities.

The claims presented for examination have been written to particularly point out the features of the invention that are not found in the prior art. Claim 1, for example, recites the step of visually displaying graphic objects on the computer display, and then selecting at least one graphic object from the displayed objects and designating it as a password graphic object. Arsenault never suggests that a displayed graphic object can be converted into a password graphic object. The claim also states that the password graphic object is applied to a further graphic object to create a password protected graphic object. Although Arsenault provides password protection for a graphic creation, it does not show nor suggest using another graphic object as a password. Nor does it teach that its password is every displayed as a graphic object. Finally, claim 1 states that the password protected graphic object cannot function unless the password graphic object is first applied as a key to unlock the password protected graphic object. Arsenault makes no such teaching, nor does the Yarsa reference. Thus it is asserted that claim 1 is patentable over the prior art.

Claim 2 as amended makes a similar recitation, except that it also recites selecting a plurality of the visually displayed graphic objects and joining them and designating them as a password graphic object. Since the reference does not teach a single graphic object password, this recitation is even more remote from Arsenault by teaching multiple graphic objects combined to form a password. Thus claim 2 is also patentable over the prior art.

Claims 3-13 all depend from claim 2, and further define that patentable method. Claims 3 and 4 state that the plurality of objects joined to form the password graphic object includes at least one (more than one in claim 4) alphanumeric characters, recognized hand drawn graphic objects, freeline hand drawn objects, and pictures. The rejection of claims 3 and 4 cites Arsenault col. 5-col. 6, but these cited portions deal with the graphic object that is password protected, NOT the nature and method of the password itself. Thus claims 3 and 4 should also be allowed. Likewise, claims 5-8 recite the use of respective colors for each password object, whereby the possible combinations that form the password object are greatly enlarged. Once again the rejection points to Arsenault, col. 5-col. 6, which describes the features of the graphic object to be protected, NOT the password structure and method. Thus claims 5-8 also define the invention over the art, and should be allowed.

Claim 9 recites the elements of the combinatorial possibilities of the password graphic object, and includes the categories of the selected objects, the colors of the selected objects, and the spatial arrangement of the selected objects that are joined to form the password graphic object. Arsenault does not make any such disclosure nor suggestion regarding the construction of a password, and claim 9 is clearly patentable over the prior art.

The rejection of claims 10 and 11 points to Arsenault col.8-col. 9, and those portions do address the structure of the protection object 220, which includes a set password method. However, Arsenault never describes making a password by combining onscreen graphic objects, and it is asserted that claims 10 and 11 are also patentable over the prior art.

Claims 12 and 13 are rejected over Arsenault and Yarsa. Although Yarsa does teach a drag-and-drop technique to apply a key icon to an encryption icon, this teaching does not bolster the inadequate Arsenault teaching, since neither reference reveals or suggests the use of the complexities of a visually displayed graphic object to form a password that has enormous combinatorial possibilities. Thus it is asserted that claims 12 and 13 should also be allowed.

All claims now presented for examination are believed to be allowable, and this application in condition for issuance. Action toward that end is earnestly solicited.

Respectfully Submitted,

Harris Zimmerman, Esq.
Registration No. 16, 437
Attorney for Applicant
Law Offices of Harris Zimmerman
1330 Broadway, Suite 710
Oakland, California 94612
(510) 465-0828

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as properly posted first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

9/20/06.

9/20/06
date